ICS-CERT MONTHLY MONITOR

OCTOBER 2011

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

CONTENTS

CYBER TIP

Work closely with both engineering and operations personnel to ensure that remotely accessed systems are correctly configured and regularly patched. When possible, minimize the exposure of these systems to the Internet by locating them behind properly configured and tested firewalls and isolated from business networks. Keep backup archives of configuration files, alarm points, switch settings as current as possible, in another physical location.

Contact Information

For any questions related to this report or to contact ICS-CERT:

E-mail: ics-cert@dhs.gov

Toll Free: 1-877-776-7585

For Control Systems Security Program (CSSP) Information and Incident Reporting:

http://www.ics-cert.org

What is ICS-CERT?

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT to:

- Conduct vulnerability and malware analysis
- Provide onsite support for incident response and forensic analysis
- Provide situational awareness in the form of actionable intelligence
- Coordinate the responsible disclosure of vulnerabilities/mitigations
- Share and coordinate vulnerability information and threat analysis through information products and alerts.

The "ICS-CERT Monthly Monitor" offers a means of promoting preparedness, information sharing, and collaboration with the 18 critical infrastructure/key resource (CIKR) sectors. ICS-CERT accomplishes this on a day-to-day basis through sector briefings, meetings, conferences, and information product releases.

This publication highlights recent activities and information products affecting industrial control systems (ICS), and provides a look ahead at upcoming ICS-related events.

DYNAMIC NATURE OF VULNERABILITY REPORTING AND DISCLOSURE

The ICS community continues to discover and respond to an ever increasing number of security issues affecting ICS products, a trend that is expected to continue into the foreseeable future. One of the distinct challenges with this upward trend is responding to a combination of common vulnerability types and those security issues that stem from the intersection of products originally designed for open connectivity with today's highly interconnected ICS environment. Regardless of the root cause, each issue identified with potential impact to ICS systems must be assessed, understood, and addressed to minimize the overall risk to critical infrastructure and key resources (CIKR) owners and operators.

ICS-CERT and the Control Systems Security Program (CSSP) recognize that processes and procedures must be dynamic and flexible to best meet the current and future needs of CIKR stakeholders. Unfortunately, no "one size fits all" approach exists to address the full spectrum of ICS vulnerabilities. For example, the most effective process to coordinate and resolve common software vulnerabilities, such as buffer overflows, will differ, in some cases substantially, from the most effective process to coordinate and resolve systemic design issues. Characteristics of each vulnerability coordination will depend on the nature of the issue reported and can result in increased coordination effort and a longer period of time to fully resolve.

Significant progress has been achieved in the ICS community regarding increased security awareness, indicated by a notable increase in the identification, reporting, and mitigation of a wide variety of control systems-related security issues. However, the fact remains that there are inherent communication-layer security challenges within the overall ICS ecosystem, many of which cannot be readily or quickly mitigated through quick-fix mechanisms such as a software patch. In order to address these much more complex, foundational, and pervasive challenges, the control systems community must work together proactively to determine the most appropriate path forward. Simply publishing alerts is not enough – we must address the root issues and decide as a community how to resolve them.

(continues on page 2)

DYNAMIC NATURE CONT.

(dynamic nature continued from page 1)

On this issue, the CSSP and ICS-CERT are engaging the CIKR constituency through a variety of initiatives. The goal is to engage with ICS stakeholders to develop effective approaches for dealing with the wide variety of ICS vulnerabilities. Two examples of these initiatives are the ICS-CERT moderated vulnerability disclosure panel discussion occurring at the upcoming Industrial Control Systems Joint Working Group (ICSJWG) Fall Conference, and the ICSJWG Cross Vendor Working Group, both of which aim to develop a unified approach for addressing these more fundamental, cross-vendor security issues that exist in industrial control systems used today.

We welcome and encourage all CIKR stakeholders to share their thoughts on these issues through involvement in the forums mentioned above or through direct input to ICS-CERT. For more information on these upcoming events, or to provide direct feedback on this topic, contact us at ICS-CERT@dhs.gov or at 1-877-756-7585.

INCIDENT RESPONSE

SCADA Hacking Using Internet Search Engines

Researchers and security experts continue to identify and report on large numbers of Internet facing ICS products and assets through freely available Internet search engines. ICS-CERT recently responded to a particular incident relating to Internet facing substations. Access to monitoring and diagnostic functions could have been exploited using a known authentication bypass vulnerability. This is but one of many examples that have been brought to the attention of ICS-CERT over the past month.

The ability to identify and directly access controllers and industrial software applications can be as simple as knowing how to search for control systems, then clicking on hyperlinks. Researchers often use freely available search engines, such as SHODAN (basic SHODAN is still free, enhanced tools version requires subscription service fees), Every Routable IP Project (ERIPP), and Google, to locate SCADA and ICS assets.[a,b] At the recent Black Hat conference, a researcher provided a Google-based search engine demonstration where an Internet facing remote terminal unit (RTU) controlling a pump station was identified.[c] Google also allows advanced searches enabled as an RSS feed, allowing a fairly continuous monitoring of assets based on a variety of search options.

Asset owners and operators can use these same tools and techniques to monitor their own industrial assets to self assess equipment installations, configuration changes, updates to firmware, software patching or upgrades, maintenance evolutions, or when contractors have conducted maintenance on their assets. While this is useful functionality for system audits, if not configured correctly, these systems may be at greater risks for cyber attacks, intrusions, and exploitation of unpatched vulnerabilities.

When these potentially susceptible systems are identified, it is important to work closely with engineering and operations personnel before attempting to resolve any Internet exposures. Industrial control systems are precisely tuned and carefully tested and designed. Configuration changes should be reviewed, approved, and tested, if possible by all stakeholders to mitigate any unintended impacts the changes may have on the system. ICS-CERT recommends that owners and operators minimize control system exposure to the Internet by locating control system networks and remote devices behind properly configured and tested firewalls.

[a] SHODAN, "Expose Online Devices," http://www.shodanhq.com/ , website last accessed October 10, 2011.

[b] Every Routable IP Project, "ERIPP," http://eripp.com/ , website last accessed October 10, 2011.

[c] gHale, "SCADA Hacking via Search Engines, ISS Source, August 4, 2011, http://www.isssource.com/scada-hacking-via-search-engines/ , website last accessed October 10, 2011.

ICS-CERT Fiscal Year 2011 Accomplishments

The number of reported cyber incidents and vulnerabilities grew in fiscal year (FY) 2011, reflecting increased public awareness of the mission criticality of ICS and the attractive targets they have become for both researchers and attackers. Reported cyber incidents tripled in FY-11, with more asset owners and operators contacting ICS-CERT for support during a cyber event. Seven of those resulted in the deployment of incident response onsite teams to assist with analysis and recovery efforts compared to five during this same time period in FY-10.

Vulnerability analysis and coordination activities were up over 700% over FY-10, with researchers using ICS-CERT as a conduit to vendors in the ICS space. Many of these issues resulted in advisories and alerts posted to the US- CERT secure portal and the public CSSP website. ICS-CERT published over 150 information products, warning the ICS community of various vulnerabilities and threats impacting control systems.

Table 1 depicts the actual statistics for the number of incidents, vulnerabilities, and fly-away events triaged and recorded by ICS-CERT in both FY-10 and FY-11.

Some of the details of these incidents and vulnerabilities have been documented in past Monthly Monitor issues; however, ICS-CERT will also provide more specific details in the 2011 ICS-CERT Annual Report that will be released in early 2012.

Table 1. ICS-CERT metrics.

ICS-CERT Metrics 2011	FY-10	FY-11
ICS Incidents	40	130
ICS Related Vulnerabilities	17	145
Incident Response Fly Away	5	7

ANNOUNCEMENTS

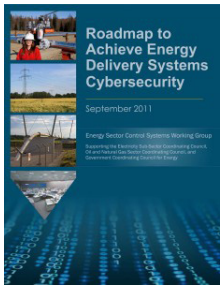
October is National Cyber Security Month

October 2011marks the 8th Annual National Cyber Security Awareness Month sponsored by the Department of Homeland Security (DHS) in cooperation with the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

http://www.dhs.gov/files/programs/gc_1158611596104.shtm

Department of Energy Releases Energy Delivery Systems Cybersecurity Roadmap

"As part of the Obama Administration's goals to enhance the security and reliability of the nation's energy infrastructure, the U.S. Department of Energy today released the 2011 *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. Developed as an update to the 2006 *Roadmap to Secure Control Systems in the Energy Sector*, today's report outlines a strategic framework over the next decade among industry, vendors, academia and government stakeholders to design, install, operate, and maintain a resilient energy delivery system capable of surviving a cyber incident while sustaining critical functions."



http://energy.gov/articles/department-energy-releases-new-roadmap-guide-public-private-cybersecurity-initiatives

(Announcements continue on page 4)

NCCIC NEWS

Fraudulent SSL Certificates

In early September, ICS-CERT became aware of the existence of fraudulent Secure Socket Layer (SSL) certificates issued by DigiNotar. An attacker could use those fraudulent SSL certificates to masquerade as legitimate sites.

Industrial control systems (ICS) that use cryptographic techniques may rely on some form of cryptographic key, whether for identification, encryption, or digital signatures. These keys are usually grouped in one location for safekeeping. Highly secure supervisory control and data acquisition (SCADA) systems using key management for the keyed system components require a certificate authority (CA) to issue the digital certificates.

The deployment of digital signatures in ICS applications is proposed in secure protocol standards such as the IEC 62351 for end-to-end SCADA protocol security methods. For owners and operators, understanding the use of the SSL in their industrial components deployment is a key to identifying the use of CAs in their control systems. Many industrial control devices today include embedded processors that support web servers and SSLs as applications; these can be found in programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices (IEDs), and other logical control devices. Operator workstations often use a version of the Windows or Linux operating systems that may also employ digital certificates. (A key component of the Stuxnet malware was the use of stolen valid certificates.) Valid certificates may also be employed in the software application automatic update process.

Control systems can be indirectly impacted through company network topology. Companies with flat networks are particularly vulnerable to the exploitation of valid certificates on business or engineering PCs and workstations, which allow threat actors easier access to control systems applications and components. Following is a list of recent updates by major vendors to address this challenge:

- Mozilla has released Firefox 3.6.22 and Firefox 6.0.2 to address this issue. Additional information can be found in the Mozilla Security Blog.
- Microsoft has removed the DigiNotar root certificates from the Microsoft Certificate Trust List. This change affects all versions of Windows Vista, Windows 7, Windows XP, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2003. Additional information can be found in Microsoft Security Advisory 2607712.
- Google Chrome users are protected from this attack due to Chrome's built-in certificate pinning feature. Google has also released Chrome 13.0.782.220 for Windows, Mac, Linux, and Chrome Frame to address this issue. Additional information can be found in the Google Security Blog and in the Google Chrome Releases blog entry.
- Adobe is releasing an update to remove the DigiNotar certificate from the Adobe Approved Trust List. In the meantime, Adobe has released a blog entry containing a work-around for Adobe Reader and Acrobat (V9 and X).

ICS-CERT encourages users and administrators to apply any necessary updates to help mitigate the risks to their systems.

ANNOUNCEMENTS

announcements continued from page 3)

ICS-CERT Control Systems Operations Center Opens its Doors

On September 29–30, 2011, DHS hosted a national media event at Idaho National Laboratory (INL) to showcase several unique cyber and control systems security capabilities that exist at this laboratory, funded and led by DHS.

The media event featured tours of several key cyber facilities including the ICS-CERT Watch floor, Control Systems Analysis Training Center, the malware lab, and sample vendor assessment bays at INL. During the tours, DHS simulated a cyber defense training exercise in which a red (attacker) team battled against a blue (defender) team to protect a bench-scale chemical plant from a cyber intrusion.

In addition to the tours, reporters were given the opportunity to conduct one-on-one interviews with senior DHS staff including Acting Deputy Under Secretary Greg Shaffer and CSSP Director Marty Edwards. Cyber Security Manager for OSIsoft, Bryan Owens, also participated in DHS Media Day by providing a vendor perspective to the media. Additional commentary for Media Day was provided by Mark Fabro, President of Lofty Perch and Mike Assante, President and CEO, National Board of Information Security Examiners.

Reporters from 11 national outlets including the New York Times, the Los Angeles Times, and National Public Radio reported on the event; CNN and FOX News did live and recorded broadcasts from the facilities in Idaho Falls, Idaho.

Media Outlets Covering Media Day

Television

- CNN—http://tinyurl.com/4y4vb5f
- FOX News—http://tinyurl.com/68uneuo

Print

- Associated Press—http://tinyurl.com/4y9bhwt
- Bloomberg News—http://tinyurl.com/6cdtnpr
- IDG News Service (Computer World, PC World)—http://tinyurl.com/3pt27do
- Los Angeles Times—http://tinyurl.com/4x67zs8
- New York Times—Story not filed as of Oct. 4, 2011
- Reuters—http://tinyurl.com/63qxnzr
- Washington Post—http://tinyurl.com/3nvctar
- Wired Magazine—http://tinyurl.com/6xflnjj.

Photo courtesy of Reuters

RECENT PRODUCT RELEASES

ALERTS

Alert "ICS-ALERT-11-271-01 - PcVue HMI/SCADA Multiple ActiveX Vulnerabilities"

ICS-CERT is aware of a public report of four vulnerabilities with proof-of-concept (PoC) exploit code affecting the PcVue HMI/SCADA Version 10.0 product. According to the report, these vulnerabilities are remotely exploitable by using an ActiveX component within a targeted machine.

Alert "ICS-ALERT-11-266-01 - Sunway Force Control Vulnerabilities"

ICS-CERT is aware of publicly available exploit code targeting multiple vulnerabilities in Sunway Force Control Version 6.1. The vulnerabilities include stack overflows, directory traversal and arbitrary file reading, and various denials-of-service vulnerabilities.

Alert "ICS-ALERT-11-256-05A - Rockwell RSLogix"

This Alert Update is a follow-up to the original ICS-CERT Alert, "ICS-ALERT-11-256-05" ROCKWELL RSLOGIX OVERFLOW VULNERABILITY," that was published September 13, 2011. ICS-CERT is aware of a public report of an overflow vulnerability with proof-of-concept (PoC) exploit code affecting the Rockwell RSLogix 5000, Version 19. According to this report, services running on Port 4446 are vulnerable to a memory overflow.

Alert "ICS-ALERT-11-256-06 - Beckhoff TwinCAT"

ICS-CERT is aware of a public report of a vulnerability with proof-of-concept (PoC) exploit code affecting Beckhoff TwinCAT, a SCADA/HMI Product. According to the report, services running on Port 48899UDP are vulnerable

Alert "ICS-ALERT-11-256-05 - Rockwell RSLogix"

ICS-CERT is aware of a public report of a overflow vulnerability with proof-of-concept (PoC) exploit code affecting the Rockwell RSLogix 19. According to this report, services running on Port 4446 are vulnerable to a memory overflow.

Alert "ICS-ALERT-11-256-04 – Measuresoft SCADAPRO Multiple Vulnerabilities"

ICS-CERT is aware of a public report of multiple vulnerabilities with proof-of-concept (PoC) exploit code affecting Measuresoft ScadaPro. According to the report, the vulnerabilities are remotely exploitable through Port 11234/UDP.

Alert "ICS-ALERT-11-256-03 - Cogent DataHub"

ICS-CERT is aware of a public report of four vulnerabilities with proof-of-concept (PoC) exploit code affecting Cogent DataHub. According to the reports, the vulnerabilities are remotely exploitable through ports that are listed in the alert.

Alert "ICS-ALERT-11-256-02 - AzeoTech DaqFactory Stack Overflow"

ICS-CERT is aware of a public report of one stack overflow vulnerability with proof-of-concept (PoC) exploit code affecting Azeotech DAQFactory, a SCADA/HMI Product. According to this report, the vulnerability is exploitable via a service running on Port 20034/UDP.

Alert "ICS-ALERT-11-256-01 - Progea Movicon - PowerHMI"

ICS-CERT is aware of a public report of three vulnerabilities with proof-of-concept (PoC) exploit code affecting Progea Movicon PowerHMI Version 11, a SCADA/HMI Product.

Alert "ICS-ALERT-11-255-01 - SCADATEC SCADAPhone ModbusTagServer"

ICS-CERT is aware of publicly released report that includes exploit code targeting a buffer overflow vulnerability in ScadaTEC SCADAPhone and ModbusTagServer products.

Alert "ICS-ALERT-11-245-01 - Multiple ActiveX Vulnerabilities in Advantech BroadWin WebAccess"

ICS-CERT has become aware of two publicly disclosed vulnerabilities with and proof-of-concept code affecting the Advantech BroadWin WebAccess Client 1.0.0.10, a web browser-based human-machine interface (HMI) product. The public disclosure indicates that these vulnerabilities are remotely exploitable. ICS-CERT has contacted and is coordinating this information with Advantech to validate and confirm this report.

ADVISORIES

Advisory "ICSA-11-273-03 - Rockwell RSLogix Denial of Service Vulnerability"

ICS-CERT is aware of a public report of a denial-of-service vulnerability in Rockwell Automations RSLogix application. Rockwell has produced a patch that mitigates this vulnerability. ICS-CERT has not tested the patch to validate that it resolves the vulnerability.

Advisory "ICSA-11-273-02 - InduSoft ISSymbol ActiveX Control Buffer Overflow"

ICS-CERT has received a report from independent security researcher Dmitriy Pletnev of Secunia Research about ActiveX control buffer overflow vulnerabilities with proof-of-concept exploit code affecting the InduSoft ISSymbol product.

Advisory "ICSA-11-273-01 - Iconics Genesis32 Multiple Memory Corruption Vulnerabilies"

Independent security researchers Billy Rios and Terry McCorkle have identified eight memory corruption vulnerabilities affecting the ICONICS GENESIS32 product. GENESIS32 is a web-deployable human-machine interface (HMI) supervisory control and data acquisition (SCADA) product.

RECENT PRODUCT RELEASES

Advisory "ICSA-11-264-01 - Azeotech DAQFactory Stack Overflow"

ICS-CERT is aware of a public report of one stack overflow vulnerability with proof-of-concept (PoC) exploit code affecting AzeoTech DAQFactory, a SCADA/HMI Product.

Advisory "ICSA-11-263-01 - Measuresoft ScadaPro"

ICS-CERT is aware of a public report of three vulnerabilities with proof-of-concept (PoC) exploit code affecting Measuresoft ScadaPro. According to the report, the vulnerabilities include a stack buffer overflow, an unsecure method call, and a path traversal, which are all remotely exploitable through Port 11234/UDP.

Advisory "ICSA-11-216-01 - Scadatec Procyon Telnet Buffer Overflow"

ICS-CERT Advisory ICSA-11-216-01P was originally released to the US-CERT Portal on August 04, 2011. This web page release was delayed to allow users sufficient time to download and install the update.

ICS-CERT has received a report from Knud Hojgaard of the nSense Vulnerability Coordination Team concerning a vulnerability in the Scadatec Limited Procyon human-machine interface/supervisory control and data acquisition (HMI/SCADA) product. This vulnerability could allow an attacker to establish a connection to the Telnet daemon, bypassing proper authentication, and exploit a buffer overflow that could lead to a denial-of-service (DoS) or remote code execution.

Advisory "ICSA-11-244-01 - Siemens WinCC flexible Runtime Heap Overflow"

ICS CERT originally released Advisory ICSA-11-244-01P on the US-CERT secure Portal on September 01, 2011. This web page release was delayed to allow users sufficient time to download and install the update.

Independent security researchers Billy Rios and Terry McCorkle have reported a memory corruption vulnerability in the WinCC Runtime Advanced Loader, which is a component of both Siemens SIMATIC WinCC flexible and TIA Portal.

ICS CERT has coordinated with Siemens and the researchers. Siemens has not issued a patch to address this vulnerability. However, Siemens has provided recommended mitigations to assist asset owners with protecting their systems.

OTHER

The ICS CERT Monthly Monitor September 2011

issue includes highlights of activities from August.

UPCOMING EVENTS

OCTOBER

NERC GridSecCon 2011

October 18–20, 2011

JW Marriott

New Orleans, LA

Industrial Control Systems Joint Working Group (ICSJWG) 2011 Fall Conference

October 24–27, 2011

Westin Long Beach Hotel

Long Beach, CA

Register for Training

NOVEMBER

2011 TSA Cyber Security in Transportation Summit

November 1–2, 2011

Sheraton Crystal City

Arlington, VA 22202

Registration: https://www.signup4.net/public/ap.aspx?EID=TSAC10E&OID=130

Contact: cybersecurity @tsa.dhs.gov

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop

(1 week)

November 7–11, 2011

Control Systems Analysis Center

Idaho Falls, ID 83415

Registration

DECEMBER

Advanced Training: Control Systems Cyber Security Advanced Training and Workshop

(1 week)

December 5–9, 2011

Control Systems Analysis Center

Idaho Falls, ID 83415

Registration

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

ICS-CERT compiles this section from multiple resources including current events as disclosed on websites, blogs, mailing lists, and at conferences. ICS-CERT does not endorse the opinions or comments stated in these articles, nor has the US Department of Homeland Security (DHS) independently verified the technical information included. The links provided were confirmed at the time of data capture. ICS-CERT is not responsible for broken or nonfunctioning URLs.

Idaho laboratory analyzed Stuxnet computer virus

September 29, 2011

Behind the doors of a nondescript red brick and gray building of Idaho National Laboratory is the malware laboratory where government cyber experts analyzed the Stuxnet computer virus.

The malicious software targets widely used industrial control systems built by German firm Siemens. Cyber experts have said it appeared aimed mostly at Iran's nuclear program and that its sophistication indicates involvement by a nation state, possibly the United States or Israel

http://www.reuters.com/article/2011/09/30/us-usa-cyber-idaho-idUSTRE78T08B20110930

AT&T says hardware failure led to outage problems with about 900 cellular towers

September 26, 2011

AT&T wireless customers in Los Angeles County are texting and making calls again after technicians fixed a widespread outage.

http://lubbockonline.com/filed-online/2011-09-26/att-says-hardware-failure-led-outage-problems-about-900-cellular-towers

DHS Thinks Some SCADA Problems Are Too Big To Call "Bug"

September 26, 2011

The Stuxnet worm may be the most famous piece of malicious software ever written. When it was first detected, a little over a year ago, the worm sounded a warning to nations around the world that critical infrastructure systems were potential targets of attack for foreign governments and cyber criminal organizations alike. But with the anniversary of the Stuxnet worm's discovery just past, the Department of Homeland Security admits that it is now reevaluating whether it makes sense to warn the public about all of the security failings of industrial control system (ICS) and SCADA software.

https://threatpost.com/en_us/blogs/dhs-thinks-some-scada-problems-are-too-big-call-bug-092611

Researcher Uncovers More SCADA Zero-Day Flaws

September 19, 2011

An Italian researcher has published details of a new batch of unpatched vulnerabilities found in the SCADA (Supervisory Control and Data Acquisition) products from seven different vendors.

Assessing the significance of the 14 zero-day vulnerabilities explained by Luigi Auriemma in proof-of-concept detail with exploit code is incredibly difficult to do, but they offer an unsettling picture of the flaws that seem to exist in systems normally hidden out of sight.

The companies mentioned include Beckhoff, MeasureSoft, Rockwell, Carel, Progea, AzeoTech, and Cogent; products used to control industrial systems across sectors including manufacturing, aerospace, military, and more or less any sector that might use SCADA.

http://www.pcworld.com/article/240197/

We Want to Hear from You

A key aspect of our mission is providing cybersecurity products and services to ICS stakeholders. As we develop and prepare new products for our customers, we want your input. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Suggestions for improving our current products are also welcome. Please help us with your feedback as we work together to meet the security challenges facing the ICS community.

If you want to see an important or pertinent topic addressed in this forum, please send your suggestions to ics-cert@dhs.gov.

DOCUMENT FAQ

What is the publication schedule for this digest?

ICS-CERT publishes the "ICS-CERT Monthly Monitor" approximately 12 times per year. Generally, each issue includes information collected in the previous 28 to 31 days.

ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets.

The public can view this document on the ICS-CERT web page at: http://www.us-cert.gov/control_systems/ics-cert/.

Please direct all questions or comments about the content, or suggestions for future content, to ICS-CERT at

ics cert@dhs.gov

OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

Targeted Attacks Not As Targeted As You Think

September 15, 2011

It's scary just how easy it is to launch sophisticated cyber attacks.

Any organization that has suffered a network infiltration and subsequent data breach will, understandably, feel as though it has been targeted by the attacker. Somehow some intruder managed to penetrate their layers of defense, usurp control of vulnerable devices and sneak off with the electronic version of their crown jewels. It is not as if the attacker was some nitwit script-kiddie that inconveniently stumbled over a vulnerability just hours before it was about to be patched, right?

http://www.esecurityplanet.com/network-security/targeted-attacks-arent-as-targeted-as-you-think.html

Federal Regulators To Investigate Blackout

September 09, 2011

Federal regulators will investigate the massive power outage that blacked out millions of customers in Southern California, Arizona, and Mexico. The Federal Energy Regulatory Commission said Friday that it will work with the North American Electric Reliability Corporation to determine what caused the blackout and how future problems can be prevented.

http://www.kpbs.org/news/2011/sep/09/federal-regulators-investigate-blackout/

Evidence of Infected SCADA Systems Washes up in Support Forums

September 06, 2011

While security experts and lawmakers debate the seriousness of cyber threats to critical infrastructure, one security researcher says that evidence that viruses and spyware already have access to industrial control systems is hiding in plain sight: on Web-based user support forums.

http://threatpost.com/en_us/blogs/evidence-infected-scada-systems-washes-support-forums-090611

COORDINATED VULNERABILITY DISCLOSURE

ICS-CERT actively works with a variety of researchers and ICS vendors to foster coordinated vulnerability disclosure. The coordinated disclosure process allows time for a vendor to release patches and users to apply patches prior to public disclosure of the vulnerability.

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US-CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact ICS-CERT at ics-cert@dhs.gov or toll free at 1-877-776-7585.

Notable Coordinated Disclosure Researchers

ICS CERT appreciates having worked through the coordinated disclosure process with the following researchers:

- Dmetriy Pletnev – Secunia Research – InduSoft ISSymbol ActiveX Control Buffer Overflow (ICSA-11-273-02 – September 30)
- Billy Rios and Terry McCorkle – Siemens WinCC Flexible Runtime Heat Overflow (ICSA-11-244-01 – September 6)
- Billy Rios and Terry McCorkle – Iconics Genesis32 Multiple Memory Corruption Vulnerabilities (ICSA-11-273-01 – September 30).

Researchers Currently Working with ICS-CERT

ICS-CERT appreciates the following researchers who continue to work through the coordinated disclosure process:

Ruben Santamarta
Kuang Chun Hung (ICST)
Jeremy Brown
Billy Rios
Joel Langill
Yun Ting Lo (ICST)
Dillon Beresford
Terry McCorkle
Carlos Mario Penagos Hollmann
Michael Orlando
Knud Erik Hojgaard (nSense)
Secunia